

LETTER

On the Nonexistence of the Ding-Helleseth-Martinsen's Constructions of Almost Difference Set for Cyclotomic Classes of Order 6

Minglong QI^{†a)}, Member, Shengwu XIONG[†], Jingling YUAN[†], Wenbi RAO[†], and Luo ZHONG[†], Nonmembers

SUMMARY Pseudorandom sequences with optimal three-level autocorrelation have important applications in CDMA communication systems. Constructing the sequences with three-level autocorrelation is equivalent to finding cyclic almost difference sets as their supports. In a paper of Ding, Helleseth, and Martinsen, the authors developed a new method known as the Ding-Helleseth-Martinsen's Constructions in literature to construct the almost difference set using product set between $GF(2)$ and union sets of cyclotomic classes of order 4. In this correspondence, we show that there do not exist such constructions for cyclotomic classes of order 6.

key words: three-level autocorrelation, the Ding-Helleseth-Martinsen's Constructions, almost difference set, cyclotomic classes of order six.

1. Introduction

Let $(A, +)$ be an Abelian group with n elements and D be a k -subset of A . Define the distance function $d_D(e) = |(D+e) \cap D|$, where $D+e = \{x+e \mid x \in D \text{ and } e \in D \setminus \{0\}\}$. D is referred to as an (n, k, λ, t) almost difference set if $d_D(e)$ takes on the value λ altogether t times and on the value $\lambda+1$ altogether $n-1-t$ times when e ranges over all the nonzero elements of A . Let $q = df+1$ be a power of an odd prime, α be a primitive element of extension field $GF(q)$. Define the cosets $D_i^{(d,q)} = \{\alpha^{kd+i} \mid 0 \leq k < f\}$, $0 \leq i < d$, which are called the cyclotomic classes of order d with respect to $GF(q)$. It is obvious that $GF(q)^* = \bigcup_{i=0}^{d-1} D_i^{(d,q)}$. The constants $(m, n)_d = |(D_m^{(d,q)} + 1) \cap D_n^{(d,q)}|$ are known as the cyclotomic numbers of order d with respect to $GF(q)$.

Pseudorandom sequences with cyclic almost difference sets as their support sets find important applications in CDMA systems [4], [5]. In [3], [5], the authors developed a new method known as the Ding-Helleseth-Martinsen's Constructions in literature to construct the almost difference set using product sets between $GF(2)$ and union sets from the cyclotomic classes of order 4. In this letter, we show that there do not exist such constructions for cyclotomic classes of order 6. The rest of the letter is structured as follows: in Section 2, the cyclotomic numbers of order 6 and their corresponding formulae are presented; in Section 3, the main theorem of the present letter is given and proved; finally a brief concluding remark is given in Section 4.

Table 1 The relations of cyclotomic numbers of order 6

(h,k)	0	1	2	3	4	5
0	(0, 0)	(0, 1)	(0, 2)	(0, 3)	(0, 4)	(0, 5)
1	(0, 1)	(0, 5)	(1, 2)	(1, 3)	(1, 4)	(1, 2)
2	(0, 2)	(1, 2)	(0, 4)	(1, 4)	(2, 4)	(1, 3)
3	(0, 3)	(1, 3)	(1, 4)	(0, 3)	(1, 3)	(1, 4)
4	(0, 4)	(1, 4)	(2, 4)	(1, 3)	(0, 2)	(1, 2)
5	(0, 5)	(1, 2)	(1, 3)	(1, 4)	(1, 2)	(0, 1)

Table 2 The cyclotomic numbers of order 6 for f even

	$m \equiv 0 \pmod{3}$	$m \equiv 1 \pmod{3}$	$m \equiv 2 \pmod{3}$
36(0, 0)	p-17-20A	p-17-8A+6B	p-17-8A-6B
36(0, 1)	p-5+4A+18B	p-5+4A+12B	p-5+4A+6B
36(0, 2)	p-5+4A+6B	p-5+4A-6B	p-5-8A
36(0, 3)	p-5+4A	p-5+4A-6B	p-5+4A+6B
36(0, 4)	p-5+4A-6B	p-5-8A	p-5+4A+6B
36(0, 5)	p-5+4A-18B	p-5+4A-6B	p-5+4A-12B
36(1, 2)	p+1-2A	p+1-2A-6B	p+1-2A+6B
36(1, 3)	p+1-2A	p+1-2A-6B	p+1-2A-12B
36(1, 4)	p+1-2A	p+1-2A+12B	p+1-2A+6B
36(2, 4)	p+1-2A	p+1+10A+6B	p+1+10A-6B

2. Cyclotomic Numbers of Order Six

Let $p = 6f+1$ be an odd prime with f even. It is well known that p can be expanded to $p = A^2 + 3B^2$. Even though there are 36 cyclotomic numbers of order 6, but there are only ten irreducible ones which can be expressed in linear combination of the vector $\langle p, A, B, 1 \rangle^T$ [1], [2]. The relations of the 36 cyclotomic numbers of order 6 with respect to the ten irreducible ones are listed in Table 1. From Table 1, it is easy to see that, for instance, $(2, 5)_6 = (1, 3)_6$. Given the prime p , and its decomposed parameters A and B , the ten distinct cyclotomic numbers of order 6 of p can be calculated by the formulae exhibited in Table 2, but there being three different sets of the formulae determined by the residue of m modulo 3, where $\alpha^m \equiv 2 \pmod{p}$ with α a primitive root of p .

3. Nonexistence of the DHM Constructions for Cyclotomic Classes of Order 6

Let \mathbb{S}_n^k denote the set of all the k -subsets of Z_n with $1 \leq k < n$. Throughout the rest of the present letter, the following notation is kept unchanged. Let $p = 6f+1$ be an odd prime with f even, $D_i^{(6,p)}$ denote the i^{th} cyclotomic class of order

[†]School of Computer Science and Technology, Wuhan University of Technology, Mafangshan West Campus, 430070 Wuhan City, China

a) E-mail: mlqiecully@163.com

DOI: 10.1587/transfun.E0.A.1

6 with $0 \leq i < 6$, $I, J \subset \mathbf{Z}_6$ be index subsets. Define $D_I = \bigcup_{i \in I} D_i^{(6,p)}$, $D_J = \bigcup_{j \in J} D_j^{(6,p)}$, $C = \{0\} \times D_I \cup \{1\} \times D_J$ and $C' = \{0\} \times D_I \cup \{1\} \times D_J \cup \{(0, 0)\}$. Define also the following distance functions

$$\begin{aligned} d_I(w) &= |(D_I + w) \cap D_I|, \\ d_{I,J}(w) &= |(D_I + w) \cap D_J|, \\ d_C(w_1, w_2) &= |(C + (w_1, w_2)) \cap C|, \\ d_{C'}(w_1, w_2) &= |(C' + (w_1, w_2)) \cap C'|, \end{aligned}$$

where $w, w_2 \in Z_p$ and $w_1 \in GF(2)$. It is clear that p can be expressed as $p = A^2 + 3B^2[1], [2]$.

The distance functions $d_C(w_1, w_2)$ and $d_{C'}(w_1, w_2)$ can be explicitly expanded out in $d_I(w_2)$, $d_J(w_2)$ and $d_{I,J}(w_2)$, stated by the following two lemmas whose proofs can be found in [3, eq.(2) and eq.(4)]

Lemma 1.

$$d_C(w_1, w_2) = \begin{cases} |D_I| + |D_J| & \text{if } w_1 = 0, w_2 = 0 \\ d_I(w_2) + d_J(w_2) & \text{if } w_1 = 0, w_2 \neq 0 \\ d_{I,J}(w_2) + d_{J,I}(w_2) & \text{if } w_1 = 1, w_2 \neq 0 \\ 2|D_I \cap D_J| & \text{if } w_1 = 1, w_2 = 0 \end{cases}$$

Lemma 2.

$$\begin{aligned} d_{C'}(w_1, w_2) &= d_C(w_1, w_2) \\ &+ \begin{cases} |D_I \cap \{w_2, -w_2\}| & \text{if } w_1 = 0, w_2 \neq 0 \\ |D_J \cap \{w_2, -w_2\}| & \text{if } w_1 = 1, w_2 \neq 0 \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

For the following lemmas and theorems of this section, let $w \in Z_p^*$ and $w^{-1} \in D_h^{(6,p)}$, denote $d_I(w)$ by $d_I(h)$ where $I \in \mathbf{Z}_6$ is an index subset.

Lemma 3. Let $I = \{0, 1, 2\} \in \mathbb{S}_6^3$. Then, the distance function $d_I(w)$ can be calculated using the following formulae:

- Case $m \equiv 0 \pmod{3}$.

$$d_I(w) = \begin{cases} \frac{p}{4} + \frac{2B}{3} - \frac{5}{4} & \text{if } w^{-1} \in D_0^{(6,p)}, \\ \frac{p}{4} - \frac{2B}{3} - \frac{1}{4} & \text{if } w^{-1} \in D_1^{(6,p)}, \\ \frac{p}{4} - \frac{1}{4} & \text{if } w^{-1} \in D_2^{(6,p)}, \\ \frac{p}{4} + \frac{2B}{3} - \frac{1}{4} & \text{if } w^{-1} \in D_3^{(6,p)}, \\ \frac{p}{4} - \frac{2B}{3} - \frac{5}{4} & \text{if } w^{-1} \in D_4^{(6,p)}, \\ \frac{p}{4} - \frac{5}{4} & \text{if } w^{-1} \in D_5^{(6,p)}. \end{cases}$$

- Case $m \equiv 1 \pmod{3}$.

$$d_I(w) = \begin{cases} \frac{p}{4} - \frac{5}{4} & \text{if } w^{-1} \in D_0^{(6,p)}, \\ \frac{p}{4} - \frac{A+B}{3} - \frac{1}{4} & \text{if } w^{-1} \in D_1^{(6,p)}, \\ \frac{p}{4} + \frac{A+B}{3} - \frac{1}{4} & \text{if } w^{-1} \in D_2^{(6,p)}, \\ \frac{p}{4} - \frac{1}{4} & \text{if } w^{-1} \in D_3^{(6,p)}, \\ \frac{p}{4} - \frac{A+B}{3} - \frac{5}{4} & \text{if } w^{-1} \in D_4^{(6,p)}, \\ \frac{p}{4} - \frac{A+B}{3} + \frac{5}{4} & \text{if } w^{-1} \in D_5^{(6,p)}. \end{cases}$$

- Case $m \equiv 2 \pmod{3}$.

$$d_I(w) = \begin{cases} \frac{p}{4} - \frac{A+B}{3} - \frac{5}{4} & \text{if } w^{-1} \in D_0^{(6,p)}, \\ \frac{p}{4} - \frac{1}{4} & \text{if } w^{-1} \in D_1^{(6,p)}, \\ \frac{p}{4} + \frac{A+B}{3} - \frac{1}{4} & \text{if } w^{-1} \in D_2^{(6,p)}, \\ \frac{p}{4} - \frac{A+B}{3} - \frac{1}{4} & \text{if } w^{-1} \in D_3^{(6,p)}, \\ \frac{p}{4} - \frac{5}{4} & \text{if } w^{-1} \in D_4^{(6,p)}, \\ \frac{p}{4} + \frac{A+B}{3} - \frac{5}{4} & \text{if } w^{-1} \in D_5^{(6,p)}. \end{cases}$$

Proof. We only prove the case $m \equiv 0 \pmod{3}$.

$$\begin{aligned} d_I(w) &= |(D_I + w) \cap D_I| \\ &= |(\bigcup_{i \in I} D_i^{(6,p)} + w) \cap (\bigcup_{j \in I} D_j^{(6,p)})| \\ &= |(\bigcup_{i \in I} (D_i^{(6,p)} + w)) \cap (\bigcup_{j \in I} D_j^{(6,p)})| \\ &= |(\bigcup_{i \in I} (w^{-1} D_i^{(6,p)} + 1)) \cap \bigcup_{j \in I} w^{-1} D_j^{(6,p)}| \\ &= |(\bigcup_{i \in I} (D_{i+h}^{(6,p)} + 1)) \cap (\bigcup_{j \in I} D_{j+h}^{(6,p)})| \\ &= \sum_{i \in I} \sum_{j \in I} |(D_{i+h}^{(6,p)} + 1) \cap D_{j+h}^{(6,p)}| \\ &= \sum_{i \in I} \sum_{j \in I} (i + h, j + h)_6 \\ &= (h, h)_6 + (h, 1 + h)_6 + (h, 2 + h)_6 + (1 + h, h)_6 + \\ &\quad (1 + h, 1 + h)_6 + (1 + h, 2 + h)_6 + (2 + h, h)_6 + \\ &\quad (2 + h, 1 + h)_6 + (2 + h, 2 + h)_6. \end{aligned} \tag{1}$$

Making varying h from 0 to 5 in the last equation of eq.(1), we can obtain the following formula. Recall that all the involved subscripts should be reduced modulo 6.

$$d_I(h) = \begin{cases} (0, 0) + (0, 1) + (0, 2) + (1, 0) + (1, 1) + \\ (1, 2) + (2, 0) + (2, 1) + (2, 2) & \text{if } h = 0; \\ (1, 1) + (1, 2) + (1, 3) + (2, 1) + (2, 2) + \\ (2, 3) + (3, 1) + (3, 2) + (3, 3) & \text{if } h = 1; \\ (2, 2) + (2, 3) + (2, 4) + (3, 2) + (3, 3) + \\ (3, 4) + (4, 2) + (4, 3) + (4, 4) & \text{if } h = 2; \\ (3, 3) + (3, 4) + (3, 5) + (4, 3) + (4, 4) + \\ (4, 5) + (5, 3) + (5, 4) + (5, 5) & \text{if } h = 3; \\ (4, 4) + (4, 5) + (4, 0) + (5, 4) + (5, 5) + \\ (5, 0) + (0, 4) + (0, 5) + (0, 0) & \text{if } h = 4; \\ (5, 5) + (5, 0) + (5, 1) + (0, 5) + (0, 0) + \\ (0, 1) + (1, 5) + (1, 0) + (1, 1) & \text{if } h = 5. \end{cases} \tag{2}$$

Remark that in eq.(2) the subscript 6 is omitted for all the cyclotomic numbers due to limited displaying. Using Table 1 to reduce all the cyclotomic numbers occurring in eq.(2) into the ten irreducible ones leads to a new form to eq.(2):

$$d_I(h) = \begin{cases} (0,0) + 2(0,1) + 2(0,2) + (0,4) + (0,5) + 2(1,2) & \text{if } h = 0; \\ (0,3) + (0,4) + (0,5) + 2(1,2) + 2(1,3) + 2(1,4) & \text{if } h = 1; \\ (0,2) + (0,3) + (0,4) + 2(1,3) + 2(1,4) + 2(2,4) & \text{if } h = 2; \\ (0,1) + (0,2) + (0,3) + 2(1,2) + 2(1,3) + 2(1,4) & \text{if } h = 3; \\ (0,0) + (0,1) + (0,2) + 2(0,4) + 2(0,5) + 2(1,2) & \text{if } h = 4; \\ (0,0) + 3(0,1) + 3(0,5) + 2(1,2) & \text{if } h = 5. \end{cases} \quad (3)$$

Last step of the proof consists of substituting the ten formulae in the first column of Table 2 for the corresponding cyclotomic numbers occurring in eq.(3) after which the assertion of Lemma 3 follows. \square

In order to compute the distance function $d_C(w_1, w_2)$ (See the beginning of Section 3) the following several lemmas are directly written down of which the proof is quite similar to that for Lemma 3 and omitted.

Lemma 4. Let $J = \{0, 4, 5\} \in \mathbb{S}_6^3$. Then, the distance function $d_J(w)$ can be calculated using the following formulae:

- Case $m \equiv 0 \pmod{3}$.

$$d_J(w) = \begin{cases} \frac{p}{4} - \frac{2B}{3} - \frac{5}{4} & \text{if } w^{-1} \in D_0^{(6,p)}, \\ \frac{p}{4} - \frac{5}{4} & \text{if } w^{-1} \in D_1^{(6,p)}, \\ \frac{p}{4} + \frac{2B}{3} - \frac{5}{4} & \text{if } w^{-1} \in D_2^{(6,p)}, \\ \frac{p}{4} - \frac{2B}{3} - \frac{1}{4} & \text{if } w^{-1} \in D_3^{(6,p)}, \\ \frac{p}{4} - \frac{1}{4} & \text{if } w^{-1} \in D_4^{(6,p)}, \\ \frac{p}{4} + \frac{2B}{3} - \frac{1}{4} & \text{if } w^{-1} \in D_5^{(6,p)}. \end{cases}$$

- Case $m \equiv 1 \pmod{3}$.

$$d_J(w) = \begin{cases} \frac{p}{4} - \frac{A+B}{3} - \frac{5}{4} & \text{if } w^{-1} \in D_0^{(6,p)}, \\ \frac{p}{4} + \frac{A+B}{3} - \frac{5}{4} & \text{if } w^{-1} \in D_1^{(6,p)}, \\ \frac{p}{4} - \frac{5}{4} & \text{if } w^{-1} \in D_2^{(6,p)}, \\ \frac{p}{4} - \frac{A+B}{3} - \frac{1}{4} & \text{if } w^{-1} \in D_3^{(6,p)}, \\ \frac{p}{4} + \frac{A+B}{3} - \frac{1}{4} & \text{if } w^{-1} \in D_4^{(6,p)}, \\ \frac{p}{4} - \frac{1}{4} & \text{if } w^{-1} \in D_5^{(6,p)}. \end{cases}$$

- Case $m \equiv 2 \pmod{3}$.

$$d_J(w) = \begin{cases} \frac{p}{4} - \frac{5}{4} & \text{if } w^{-1} \in D_0^{(6,p)}, \\ \frac{p}{4} + \frac{A-B}{3} - \frac{5}{4} & \text{if } w^{-1} \in D_1^{(6,p)}, \\ \frac{p}{4} - \frac{A-B}{3} - \frac{5}{4} & \text{if } w^{-1} \in D_2^{(6,p)}, \\ \frac{p}{4} - \frac{1}{4} & \text{if } w^{-1} \in D_3^{(6,p)}, \\ \frac{p}{4} + \frac{A-B}{3} - \frac{1}{4} & \text{if } w^{-1} \in D_4^{(6,p)}, \\ \frac{p}{4} - \frac{A-B}{3} - \frac{1}{4} & \text{if } w^{-1} \in D_5^{(6,p)}. \end{cases}$$

Lemma 5. Let $I = \{0, 1, 2\} \in \mathbb{S}_6^3$ and $J = \{0, 4, 5\} \in \mathbb{S}_6^3$. Then, the distance function $d_{I,J}(w)$ can be calculated using the following formulae:

- Case $m \equiv 0 \pmod{3}$.

$$d_{I,J}(w) = \begin{cases} \frac{p}{4} - \frac{A}{3} - \frac{11}{12} & \text{if } w^{-1} \in D_0^{(6,p)}, \\ \frac{p}{4} + \frac{A+B}{6} - \frac{5}{12} & \text{if } w^{-1} \in D_1^{(6,p)}, \\ \frac{p}{4} + \frac{A-B}{6} - \frac{5}{12} & \text{if } w^{-1} \in D_2^{(6,p)}, \\ \frac{p}{4} - \frac{A}{3} + \frac{1}{12} & \text{if } w^{-1} \in D_3^{(6,p)}, \\ \frac{p}{4} + \frac{A+B}{6} - \frac{5}{12} & \text{if } w^{-1} \in D_4^{(6,p)}, \\ \frac{p}{4} + \frac{A-B}{6} - \frac{5}{12} & \text{if } w^{-1} \in D_5^{(6,p)}. \end{cases}$$

- Case $m \equiv 1 \pmod{3}$.

$$d_{I,J}(w) = \begin{cases} \frac{p}{4} + \frac{B}{3} - \frac{11}{12} & \text{if } w^{-1} \in D_0^{(6,p)}, \\ \frac{p}{4} + \frac{A-3B}{6} - \frac{5}{12} & \text{if } w^{-1} \in D_1^{(6,p)}, \\ \frac{p}{4} - \frac{A-B}{6} - \frac{5}{12} & \text{if } w^{-1} \in D_2^{(6,p)}, \\ \frac{p}{4} + \frac{B}{3} + \frac{1}{12} & \text{if } w^{-1} \in D_3^{(6,p)}, \\ \frac{p}{4} + \frac{A-3B}{6} - \frac{5}{12} & \text{if } w^{-1} \in D_4^{(6,p)}, \\ \frac{p}{4} - \frac{A-B}{6} - \frac{5}{12} & \text{if } w^{-1} \in D_5^{(6,p)}. \end{cases}$$

- Case $m \equiv 2 \pmod{3}$.

$$d_{I,J}(w) = \begin{cases} \frac{p}{4} - \frac{B}{3} - \frac{11}{12} & \text{if } w^{-1} \in D_0^{(6,p)}, \\ \frac{p}{4} - \frac{A+B}{6} - \frac{5}{12} & \text{if } w^{-1} \in D_1^{(6,p)}, \\ \frac{p}{4} + \frac{A+3B}{6} - \frac{5}{12} & \text{if } w^{-1} \in D_2^{(6,p)}, \\ \frac{p}{4} - \frac{B}{3} + \frac{1}{12} & \text{if } w^{-1} \in D_3^{(6,p)}, \\ \frac{p}{4} - \frac{A+B}{6} - \frac{5}{12} & \text{if } w^{-1} \in D_4^{(6,p)}, \\ \frac{p}{4} + \frac{A+3B}{6} - \frac{5}{12} & \text{if } w^{-1} \in D_5^{(6,p)}. \end{cases}$$

Lemma 6. Let $I = \{0, 1, 2\} \in \mathbb{S}_6^3$ and $J = \{0, 4, 5\} \in \mathbb{S}_6^3$. Then, $d_{I,J}(w) = d_{J,I}(w)$ for $w \in Z_p^*$.

Now, we are ready to compute the distance function $d_C(w_1, w_2)$.

Lemma 7. Let $I = \{0, 1, 2\} \in \mathbb{S}_6^3$ and $J = \{0, 4, 5\} \in \mathbb{S}_6^3$. Then, the distance function, $d_C(w_1, w_2) = |(C + (w_1, w_2)) \cap C|$, can be calculated by the following formulae:

- Case $m \equiv 0 \pmod{3}$.

$$- w_1 = 0.$$

$$d_C(w_1, w_2) = \begin{cases} \frac{p-5}{2} & \text{if } w_2^{-1} \in D_0^{(6,p)}, \\ \frac{3p-4B-9}{6} & \text{if } w_2^{-1} \in D_1^{(6,p)}, \\ \frac{3p+4B-9}{6} & \text{if } w_2^{-1} \in D_2^{(6,p)}, \\ \frac{p-1}{2} & \text{if } w_2^{-1} \in D_3^{(6,p)}, \\ \frac{3p-4B-9}{6} & \text{if } w_2^{-1} \in D_4^{(6,p)}, \\ \frac{3p+4B-9}{6} & \text{if } w_2^{-1} \in D_5^{(6,p)}. \end{cases}$$

$$- w_1 = 1.$$

$$d_C(w_1, w_2) = \begin{cases} \frac{3p-4A-11}{6} & \text{if } w_2^{-1} \in D_0^{(6,p)}, \\ \frac{3p+2A+2B-5}{6} & \text{if } w_2^{-1} \in D_1^{(6,p)}, \\ \frac{3p+2A-2B-5}{6} & \text{if } w_2^{-1} \in D_2^{(6,p)}, \\ \frac{3p-4A+1}{6} & \text{if } w_2^{-1} \in D_3^{(6,p)}, \\ \frac{3p+2A+2B-5}{6} & \text{if } w_2^{-1} \in D_4^{(6,p)}, \\ \frac{3p+2A-2B-5}{6} & \text{if } w_2^{-1} \in D_5^{(6,p)}. \end{cases}$$

– $w_1 = 1$ and $w_2 = 0$.

$$d_C(w_1, w_2) = \frac{p-1}{3}.$$

• Case $m \equiv 1 \pmod{3}$.

– $w_1 = 0$.

$$d_C(w_1, w_2) = \begin{cases} \frac{3p-2A-2B-15}{6} & \text{if } w_2^{-1} \in D_0^{(6,p)}, \\ \frac{p-3}{2} & \text{if } w_2^{-1} \in D_1^{(6,p)}, \\ \frac{3p+2A+2B-9}{6} & \text{if } w_2^{-1} \in D_2^{(6,p)}, \\ \frac{3p-2A-2B-3}{6} & \text{if } w_2^{-1} \in D_3^{(6,p)}, \\ \frac{p-3}{2} & \text{if } w_2^{-1} \in D_4^{(6,p)}, \\ \frac{3p+2A+2B-9}{6} & \text{if } w_2^{-1} \in D_5^{(6,p)}. \end{cases}$$

– $w_1 = 1$.

$$d_C(w_1, w_2) = \begin{cases} \frac{3p+4B-11}{6} & \text{if } w_2^{-1} \in D_0^{(6,p)}, \\ \frac{3p+2A-6B-5}{6} & \text{if } w_2^{-1} \in D_1^{(6,p)}, \\ \frac{3p-2A+2B-5}{6} & \text{if } w_2^{-1} \in D_2^{(6,p)}, \\ \frac{3p+4B+1}{6} & \text{if } w_2^{-1} \in D_3^{(6,p)}, \\ \frac{3p+2A-6B-5}{6} & \text{if } w_2^{-1} \in D_4^{(6,p)}, \\ \frac{3p-2A+2B-5}{6} & \text{if } w_2^{-1} \in D_5^{(6,p)}. \end{cases}$$

– $w_1 = 1$ and $w_2 = 0$.

$$d_C(w_1, w_2) = \frac{p-1}{3}.$$

• Case $m \equiv 2 \pmod{3}$.

– $w_1 = 0$.

$$d_C(w_1, w_2) = \begin{cases} \frac{3p-2A+2B-15}{6} & \text{if } w_2^{-1} \in D_0^{(6,p)}, \\ \frac{3p+2A-2B-9}{6} & \text{if } w_2^{-1} \in D_1^{(6,p)}, \\ \frac{p-3}{2} & \text{if } w_2^{-1} \in D_2^{(6,p)}, \\ \frac{3p-2A+2B-3}{6} & \text{if } w_2^{-1} \in D_3^{(6,p)}, \\ \frac{3p+2A-2B-9}{6} & \text{if } w_2^{-1} \in D_4^{(6,p)}, \\ \frac{p-3}{2} & \text{if } w_2^{-1} \in D_5^{(6,p)}. \end{cases}$$

– $w_1 = 1$.

$$d_C(w_1, w_2) = \begin{cases} \frac{3p-4B-11}{6} & \text{if } w_2^{-1} \in D_0^{(6,p)}, \\ \frac{3p-2A-2B-5}{6} & \text{if } w_2^{-1} \in D_1^{(6,p)}, \\ \frac{3p+2A+6B-5}{6} & \text{if } w_2^{-1} \in D_2^{(6,p)}, \\ \frac{3p-4B+1}{6} & \text{if } w_2^{-1} \in D_3^{(6,p)}, \\ \frac{3p-2A-2B-5}{6} & \text{if } w_2^{-1} \in D_4^{(6,p)}, \\ \frac{3p+2A+6B-5}{6} & \text{if } w_2^{-1} \in D_5^{(6,p)}. \end{cases}$$

– $w_1 = 1$ and $w_2 = 0$.

$$d_C(w_1, w_2) = \frac{p-1}{3}.$$

Proof. The actual lemma can be proved by using Lemma 1 as the leading lemma and Lemmas 2-6 as auxiliary lemmas. \square

Lemma 8. Let $I = \{0, 1, 2\} \in \mathbb{S}_6^3$ and $J = \{0, 4, 5\} \in \mathbb{S}_6^3$. Define $D_I = \bigcup_{i \in I} D_i^{(6,p)}$, $D_J = \bigcup_{j \in J} D_j^{(6,p)}$, $C = \{0\} \times D_I \cup \{1\} \times D_J$. Then, C cannot form an almost difference set over $GF(2) \times Z_p$.

Proof. Lemma 7 gives the distance function $d_C(w_1, w_2)$. Its value distribution according to all the cases of w_2 is so irregular that the condition of forming the almost difference set specified in Section 1 cannot be fulfilled for whatever are the parameters A and B . \square

Lemma 9. Let $I, J \in \mathbb{S}_6^3$, $D_I = \bigcup_{i \in I} D_i^{(6,p)}$, $D_J = \bigcup_{j \in J} D_j^{(6,p)}$, and $C = \{0\} \times D_I \cup \{1\} \times D_J$. Then, C cannot form an almost difference set over $GF(2) \times Z_p$.

Proof. For each pair of subscript sets $(I, J) \in \mathbb{S}_6^3 \times \mathbb{S}_6^3$, the distance function $d_C(w_1, w_2)$ can be computed out as for Lemma 9. Computational results show that there are no pair of subscript sets $(I, J) \in \mathbb{S}_6^3 \times \mathbb{S}_6^3$ such that C forms an almost difference set over $GF(2) \times Z_p$. \square

Lemma 10. Let $I, J \in \mathbb{S}_6^k$ where $1 \leq k < 6$, $D_I = \bigcup_{i \in I} D_i^{(6,p)}$, $D_J = \bigcup_{j \in J} D_j^{(6,p)}$, and $C = \{0\} \times D_I \cup \{1\} \times D_J$. Then, C cannot form an almost difference set over $GF(2) \times Z_p$.

Proof. Similar to the proof for Lemma 9. \square

Lemma 11. Let $p = 12f + 1$ be an odd prime, and $I \in \mathbb{S}_6^k$ with $1 \leq k < 6$. If $D_0^{(6,p)} \subset D_I$ then $\delta_I = |D_I \cap \{w_2, -w_2\}| = 2$, else $\delta_I = |D_I \cap \{w_2, -w_2\}| = 0$. Where $w_2 \in Z_p^*$.

Proof. It is obvious. \square

Lemma 12. Let $I, J \in \mathbb{S}_6^k$ where $1 \leq k < 6$, $D_I = \bigcup_{i \in I} D_i^{(6,p)}$, $D_J = \bigcup_{j \in J} D_j^{(6,p)}$, and $C' = \{0\} \times D_I \cup \{1\} \times D_J \cup \{(0, 0)\}$. Then, C' cannot form an almost difference set over $GF(2) \times Z_p$.

Proof. The present lemma can be proved by using Lemma 2 as the leading lemma and Lemma 10, Lemma 11 as auxiliary lemmas. \square

We are now at the step to be able to assert whether or not there exist the DHM Constructions for the cyclotomic classes of order 6.

Theorem 1. Let $p = 12f + 1$ be an odd prime, and suppose that $p = A^2 + 3B^2$. Then, there are no the DHM Constructions of the almost difference set from product sets between $GF(2)$ and union sets of cyclotomic classes of order 6 for the prime p .

Proof. By Lemma 10 and Lemma 12. \square

4. Conclusion

Pseudorandom sequences with optimal three-level autocorrelation have important applications in CDMA communication. Constructing such sequences is equivalent to finding

cyclic almost difference sets as their supports. The Ding-Helleseth-Martinsens Constructions is an efficient method to construct the almost difference set. In this letter it is shown that there are no such constructions for the cyclotomic classes of order 6.

References

- [1] L. E. Dickson, "Cyclotomy, higher congruence and Waring's problem," *Amer. J. Math.*, vol. 57, pp. 391-424, 1935.
- [2] A. L. Whiteman, "The cyclotomic numbers of order twelve," *Acta Arith.*, vol. 6, pp. 537-60, 1960.
- [3] C. Ding, T. Helleseht, H. Martinsen, "New families of binary sequences with optimal three-level autocorrelation," *IEEE Trans. Inform. Theory*, vol. 47, no. 1, pp. 428-433, 2001.
- [4] C. Ding, T. Helleseht, K. Y. Lam, "Several classes of sequences with three-level autocorrelation," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2606-2612, 1999.
- [5] K. T. Arasu, C. Ding, T. Helleseht, P. V. Kumar, H. M. Martinsen, "Almost difference sets and their sequences with optimal autocorrelation," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2934-2943, 2001.